AF/IFW

TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No.
ITL.0667US

In Re Application Of: **Kelan C. Silvester**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/974,923	October 10, 2001	Carl G. Colin	21906	2136	1093

Invention: **Using a Communication Protocol to Provide Security Services**

COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on **January 11, 2006**

The fee for filing this Appeal Brief is: **$500.00**

☒ A check in the amount of the fee is enclosed.

□ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **20-1504**

□ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **February 20, 2006**

Timothy N. Trop, Reg. No. 28,994
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Suite 100
Houston, TX 77024
713/468-8880 [Phone]
713/468-8883 [Fax]

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

February 20, 2006.
(Date)

Signature of Person Mailing Correspondence

Nancy Meshkoff
Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Applicant:		§		
	Kelan C. Silvester	§	Art Unit:	2136
		§		
Serial No.:	09/974,923	§	Examiner:	Carl G. Colin
		§		
Filed:	October 10, 2001	§	Atty Docket:	ITL.0667US (P12985)
		§		
For:	Using a Communication Protocol to Provide Security Services	§		
		§	Assignee:	Intel Corporation
		§		

Mail Stop **Appeal Brief-Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Date of Deposit: February 20, 2006
I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Nancy Meshkoff

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is the assignee Intel Corporation.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-5 and 7-29 (Rejected).
Claim 6 (Canceled).

Claims 1-5 and 7-29 are rejected and are the subject of this Appeal Brief.

STATUS OF AMENDMENTS

There is one pending unentered amendment filed February 16, 2006.

SUMMARY OF CLAIMED SUBJECT MATTER

In the following discussion, the independent claims are read on one of many possible embodiments without limiting the claims:

1. A method comprising:

disabling an operation of a wireless device (14) that fails to communicate with a base station over a range limited wireless protocol (Specification at page 3, line 22 to page 4, line 2.

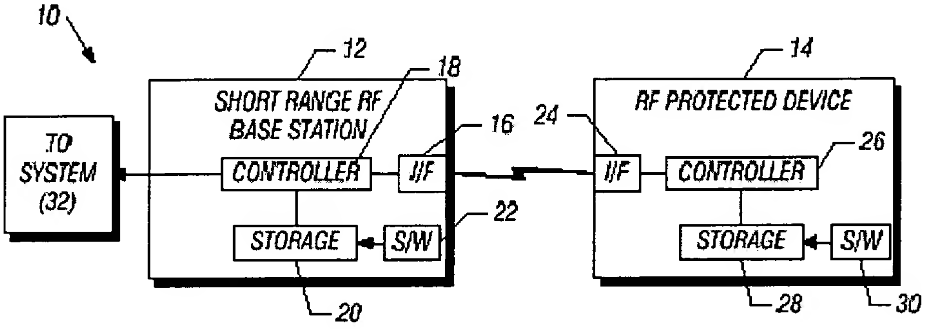

FIG. 1

3. The method of claim 2 wherein sending a short range wireless signal includes sending a Bluetooth protocol signal.

10. The method of claim 1 including preventing the device (14) from booting if the signal is not authenticated by said base station (12) (See Figure 1, specification at page 4, lines 4-6).

11. A portable wireless device comprising:

a processor (26, Figure 1);

a wireless receiver (24, Figure 1); and

a storage (28, Figure 1) coupled to said processor, said storage storing instructions that enable the processor to disable an operation of a wireless device that fails to communicate with a base station over a range limited wireless protocol (Specification at page 3, line 22 to page 4, line 20).

13. The device of claim 12 wherein said receiver is a Bluetooth protocol transceiver.

19. The device of claim 11 wherein said device prevents the device (14) from booting if the signal is not authenticated (See Figure 1, specification at page 4, lines 4-6).

20. An article comprising a medium storing instructions that enable a processor-based system to:

send a wireless signal from a portable device (Figure 2, 14) to a base station (page 5, lines 3-5); and

disable an operation of the device that fails to communicate with a base station over a range limited wireless protocol (page 5, lines 10-16).

22. The article of claim 21 further storing instructions that enable the processor-based system to receive a Bluetooth protocol signal.

29. An article of claim 20 further storing instructions that enable the processor-based system to prevent the device (14) from booting if the signal is not authenticated (See Figure 1, specification at page 4, lines 4-6).

At this point, no issue has been raised that would suggest that the words in the claims have any meaning other than their ordinary meanings. Nothing in this section should be taken as an indication that any claim term has a meaning other than its ordinary meaning.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Are claims 1-2, 4, 7-9, 11-12, 14, 16-18, 20-21, 23, and 26-28 anticipated by Cromer?

B. Are claims 3, 10, 13, 19, 22, and 29 unpatentable over Cromer in view of Girard?

ARGUMENT

A. Are claims 1-2, 4, 7-9, 11-12, 14, 16-18, 20-21, 23, and 26-28 anticipated by Cromer?

Claim 1 calls for disabling an operation of wireless device that "fails to communicate with a base station over a limited wireless protocol."

Cromer only teaches disabling in the face of failure to authenticate. In the final rejection, the Examiner admits as much. Moreover, the Examiner now concedes that he is not relying on the GPS embodiment of Cromer. See the advisory action.

Therefore, the only basis for the rejection is that a failure to be authenticated amounts to a failure to communicate. But, necessarily, an authentication failure involves a communication. An authentication failure necessarily includes trying to communicate and being rejected, after communicating, for not being within the class of devices that are allowed to communicate.

Thus, the rejection is not commensurate with the claims. The claims require that the failure to communicate be the basis for disabling an operation. The reference teaches that when authentication is denied, then communications would be cut off.

The Examiner asserts that the applicant is distinguishing a GPS embodiment, not another embodiment that the Examiner is relying upon. The Examiner cites column 8, lines 23-28, in the final rejection at paragraph 2.2. That language is in the reference's claims. It calls for disabling a portable computer in response to the portable computer being moved outside an authorized area for use. The only way that the cited reference teaches determining that something is outside the area of use is in response to a GPS determination. Nothing else is cited.

It is further suggested that a portable computer may be located within a room or building controlled by a gate that meets the recitation of a base station which includes a wireless transmitter/receiver for transmitting information to/from the portable computer from the gate. A bunch of things are cited, but none of them have anything to do with disabling an operation in response to a failure to communicate.

Column 3, lines 21-26, merely talks about authorized geographic area.

Column 3, line 61, through column 4, line 16, talks about a security unit determining whether a password is correct. But for the computer system to determine whether the password is correct it has to have a communication. Thus, cutting off communications in response to a failure of a password is not cutting off communications in response to a failure of communications, it is cutting off communications in response to a completion of communications, but the failure to properly be authenticated.

Column 4, lines 34-42, is also cited. Again, this talks about the failure to be authorized, which necessarily entails actually completing a communication. Plainly, the cited reference is exactly the opposite of what is claimed. It requires a communication in order to disable communications and never disables communications in response to any failure to communicate. The same effect is cited in column 5, lines 57-65. Again, this speaks of a password and the receipt of a password which necessarily requires a communication.

Claim 1 calls for disabling an operation of a wireless device that "fails to communicate with a base station over a range limited wireless protocol." Here, there is no failure to communicate and no disabling of an operation in response. To the contrary, there is a completed communication and, upon the failure to provide the correct password, some type of disabling. Plainly, the cited reference fails to teach the claimed limitations.

It is believed that the Examiner concedes that, necessarily, the GPS embodiment, as the Examiner talks of it in the advisory action, necessarily fails to meet the claimed limitation.

Therefore, the rejection should be reversed.

B. Are claims 3, 10, 13, 19, 22, and 29 unpatentable over Cromer in view of Girard?

Claim 10 is rejected over Cromer in view of Girard. It is argued that Girard teaches wirelessly locking a computer platform to discourage theft. It is suggested that Cromer discloses starting booting and discloses "the gate" authenticating the base station to allow "next booted". It is not clear what is meant by this language, but, by the examiner's own language, it appears that what Cromer and Girard teach cannot relate to the claim. For example, even if Girard "discloses pre-boot authentication code to access the system authentication". There is nothing which requires that a device be authenticated to send a signal to the base station and, if the base station does not authenticate the signal, the wireless device itself cannot boot.

In other words, the claim is more limited than simply requiring authentication. It requires authentication involving a signal sent from the wireless device to the base station and further it requires authentication by the base station to allow the sending wireless device to boot. No such operation is anywhere suggested in any of the material relied upon.

For example, the material cited in column 5, lines 41-55 talks about authentication, but this does not reach the scope of the claimed invention which involves a very special kind of authentication nowhere contemplated in the cited reference.

Therefore the rejection should be reversed.

Moreover, the present application and the Girard patent were, at the time the invention of the present application was made, owned by Intel Corporation. Therefore Girard cannot be combined with another reference under § 103(c).

Applicant respectfully requests that each of the final rejections be reversed and that the claims subject to this Appeal be allowed to issue.

Respectfully submitted,

Date: 2/17/06

Timothy N. Trop, Reg. No. 28,994
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Ste. 100
Houston, TX 77024
713/468-8880 [Phone]
713/468-8883 [Fax]

Attorneys for Intel Corporation

CLAIMS APPENDIX

The claims on appeal are:

1. A method comprising:

disabling an operation of a wireless device that fails to communicate with a base station over a range limited wireless protocol.

2. The method of claim 1 including sending a short-range wireless signal from said wireless device to said base station.

3. The method of claim 2 wherein sending a short range wireless signal includes sending a Bluetooth protocol signal.

4. The method of claim 1 wherein preventing operation of the device includes preventing access to a supply of power.

5. The method of claim 1 including sending a wireless signal from said wireless device to a key fob.

7. The method of claim 1 including preventing operation of the device if the signal is not authenticated by said base station.

8. The method of claim 1 including adversely affecting the performance of the device if the signal is not authenticated by said base station.

9. The method of claim 1 including limiting access to storage if the signal is not authenticated by said base station.

10. The method of claim 1 including preventing the device from booting if the signal is not authenticated by said base station.

11. A portable wireless device comprising:

a processor;

a wireless receiver; and

a storage coupled to said processor, said storage storing instructions that enable the processor to disable an operation of a wireless device that fails to communicate with a base station over a range limited wireless protocol.

12. The device of claim 11 wherein said receiver receives a short-range wireless signal.

13. The device of claim 12 wherein said receiver is a Bluetooth protocol transceiver.

14. The device of claim 11 wherein said processor to prevent operation of the device by preventing access to a supply of power.

15. The device of claim 11 wherein said device is in the form of a key fob.

16. The device of claim 11 to prevent operation of the device if the device sending a wireless signal is not authenticated.

17. The device of claim 11 wherein said device adversely affects the performance of the device if the signal is not authenticated.

18. The device of claim 11 wherein said device limits access to storage if the signal is not authenticated.

19. The device of claim 11 wherein said device prevents the device from booting if the signal is not authenticated.

20. An article comprising a medium storing instructions that enable a processor-based system to:

send a wireless signal from a portable device to a base station; and

disable an operation of the device that fails to communicate with a base station over a range limited wireless protocol.

21. The article of claim 20 further storing instructions that enable the processor-based system to receive a short-range wireless signal.

22. The article of claim 21 further storing instructions that enable the processor-based system to receive a Bluetooth protocol signal.

23. The article of claim 20 further storing instructions that enable the processor-based system to prevent access to a supply of power.

24. The article of claim 20 further storing instructions that enable the processor-based system to receive a wireless signal at a key fob.

25. The article of claim 20 further storing instructions that enable the processor-based system to receive a wireless signal at a concealed location.

26. An article of claim 20 further storing instructions that enable the processor-based system to prevent operation of the device if the signal is not authenticated.

27. An article of claim 20 further storing instructions that enable the processor-based system to adversely affect the performance of the device if the signal is not authenticated.

28. An article of claim 20 further storing instructions that enable the processor-based system to limit access to storage if the signal is not authenticated.

29. An article of claim 20 further storing instructions that enable the processor-based system to prevent the device from booting if the signal is not authenticated.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.